Please rewrite the paragraph on page 2, lines 26-32 as shown:

B2

NON-LIABILITY - Particularly when communicating over a public communication system, there are occasions when communication is interrupted, or a message is not confirmed as having been received, or a computer system crashes. In such a situation, it may be impossible to establish whether an instructed electronic money transaction or transfer has taken place. In other situations, data representing the electronic money might be lost. It is desirable that an electronic money user [~~to~~] be able to repeat the same transaction, or make "back-up" copies of the electronic money, without increasing the liability of the user and the bank.

Please rewrite the paragraph on page 9, lines 24-30 as shown:

B3

Such a technique achieves complete security for the new bearer even though the new value note will be handled by the original bearer. The new bearer will be able to verify the authenticity of the new value note independently by means of the value note issuer's signature. Furthermore, it will be impossible for the original bearer to attempt to forge the new bearer's signature because the original bearer will only be aware of the new bearer's public key; the original bearer will not be aware of the new bearer's secret key which is required for writing an endorsement signature.

Please rewrite the paragraph on page 24, lines 18-31 as shown:

B4

The next step (step 76 in Fig. 7) is for the buyer to append payment instruction information 68 to the value note 20 (Fig. 2), to form new value

note 21 as illustrated in Fig. 6. In the present example, the payment instruction information instructs the bank to split the money value of the original value note 20 (Fig. 2) between the new value note 50 for the seller, and the new value note 60 for the buyer. The payment instruction information can identify each of the new value notes 50 and 60 by means of the bearer's reference 56 and 66, respectively. Also in this example, the respective currency values have been included in the seller's new value note 50, the buyer's new value note 60, as well as in the payment instruction information 68. This redundancy may be useful to ensure that no errors or mistakes occur in the new value note and the payment instruction information. However, the information might instead be included only once, either in the payment instruction information 68, the buyer's new value note 60, or the seller's new value note 50. For example, the bank computer 10 would be able to calculate the necessary "change" from the original value information 24 and the payment value 54 from the seller's new value note 50.

Please rewrite the paragraph on page 25, lines 15-32 as shown:

Having "signed" the value note 21, the buyer would then transmit the endorsed value note 21, the blank new buyer's value note 60 and the blank new seller's value note 50 through the communication network 14 to the bank computer 10 (step 78 in Fig. 7). The endorsed value note, and the blank value notes, may either be transmitted in their entirety or, alternatively, only selected information might be transmitted. For example, since each value note has its own unique identification number, the entire information in the value note does not itself need to be transmitted back to the issuing authority (the issuing authority will be able

to access such information from their record copy of the original value note and, indeed, would normally access this information to verify the redemption instructions). In its briefest form, the instructions may be transmitted without any information from the original value note apart from the identification number. The instructions may also simply include a reference number and public key for each new value note to be generated (instead of transmitting a whole blank value note). An instruction format using such "reduced" information is described in more detail later; the current description is to be interpreted to cover using such "reduced" or short-hand information as well as transmitting full information. It is emphasised that the use of "reduced" information does not limit the information which can be included in the endorsing signature, since this can be based on all of the value information (such information being available to both the bearer and the money handling authority).

B5 cont

Please rewrite the paragraph on page 26, lines 1-5 as shown:

Referring to Fig. 8, the bank computer performs a number of verification tests upon the endorsed value note 21 (Fig. 6) to determine its authenticity. The order in which the tests are performed is not important; if any one of the tests fails, then the bank computer 10 may treat the value note as being "false", and need not honour the value note.

B6

Please rewrite the paragraph on page 26, lines 7-10 as shown:

In this example, the bank computer 10 first performs a test 80 upon the "valid from" date information 34 and the expiry date information 36 in the received original value note 20 (Fig. 2), (or in the copy of the note

B7

B7 Cont

already held by the bank computer if the original note is not returned) to ascertain whether the current date falls within an allowable window.

Please rewrite the paragraph on page 26, lines 12-18 as shown:

B8

Assuming that the date is satisfactory, the bank computer 10 next proceeds to step 82 at which the buyer's signature 70 is analysed. By using the public key information 22 originally presented in the value note 20 (Fig. 2), the bank computer 10 attempts to verify that the signature information 70 matches the information in the endorsed value note 21 upon which the signature information 70 is based. As explained above, the signature information 70 depends at least upon the payment instruction information 68, and may also depend on other predetermined information in the value note.

Please rewrite the paragraph on page 26, line 27 through page 27, line 4 as shown:

B9

At step 92 (in Fig. 8), the bank computer 10 completes the endorsed original value note 21 to provide a receipt of the transaction to the buyer. The completed original value note 67 is illustrated in Fig. 11. This includes an "OK" message indicated at 94, and a final bank signature 96. The final bank signature is calculated based on the text of the buyer's signature 70 described above, and acts as a guarantee that the buyer's signature cannot subsequently be altered, either by the bank or by the buyer, should a dispute arise later. As indicated in Fig. 11, the final bank signature 96 may also be based on other information in the value note 67, such as the "valid from" information 32 (Fig. 2), the payment

B9 Cont

instruction information 68 (Fig. 6), and the "OK" message 94, to prevent alteration of those items of information in case of a dispute later.

Please rewrite the paragraph on page 27, lines 6-12 as shown:

B10

If the above tests 80, 82 and 84 are all satisfied, this is indicative that the completed original value note 67 has not been tampered with, and that the buyer is the correct bearer authorised to redeem the value note. The next test 86 performed by the bank computer 10 ascertains whether the value note 67 has previously been redeemed. This test can be performed by comparing the bank's reference code 30 (Fig. 2) in the completed original value note 67 with a list maintained in the bank computer 10 of each value note and the date, if any, of redemption. The purpose of this test 86 is to prevent a user from "double spending" a value note.

Please rewrite the paragraph on page 27, lines 14-20 as shown:

B11

Assuming that the value note 67 has not previously been redeemed, the bank computer records the current date as the date of redemption, and proceeds to step 88 at which the new seller's value note 50 is completed and a bank's signature added to authenticate the new value note 50 in the same manner as that described above for the value note 20. The completed seller's value note is illustrated in Fig. 9. This is similar to the original form of value note 20 shown in Fig. 2, and the same reference numerals (followed by the letter "s") are used to indicate the corresponding information in the completed value note 50s.

Please rewrite the paragraph on page 27, lines 22-25 as shown:

B/2

Similarly, at step 90 (in Fig. 8), the new buyer's value note 60 is completed and a bank's signature is added to authenticate the new buyer's value note 60. The completed new buyer's value note 60b is illustrated in Fig. 10, and corresponding reference numerals (followed by the letter "b") denote the value note information described previously.

Please rewrite the paragraph on page 27, line 27 through page 28, line 3 as shown:

B/3

At step 92 (in Fig. 8), the bank computer 10 completes the original value note 20 to provide a receipt of the transaction to the buyer. The completed original value note 67 is illustrated in Fig. 11. This includes an "OK" message indicated at 94, and a final bank signature 96. The final bank signature is calculated based on the text of the buyer's signature 70 described above, and acts as a guarantee that the buyer's signature cannot subsequently be altered, either by the bank or by the buyer, should a dispute arise later. As indicated in Fig. 11, the final bank signature 96 may also be based on other information in the value note 67, such as the "valid from" information 32 (Fig. 2), the payment instruction information 68 (Fig. 6), and the "OK" message 94, to prevent alteration of those items of information in case of a dispute later.

Please rewrite the paragraph on page 28, lines 5-12 as shown.

B/4

Finally, at step 98 (in Fig. 8), the bank computer 10 transmits the new seller's value note 50s, the new buyer's new value note 60b and the completed original value note 67 to the buyer's computer terminal. This is

B14 Cont

the computer terminal from which the original transaction instructions were transmitted to the bank computer 10. Upon receipt of the new value notes, the buyer would keep his own new value note 60b for further use, and forward the new seller's value note 50s to the seller as payment. The buyer's computer terminal would typically communicate with the seller's computer terminal through the public communication system 14 to transfer the seller's value note 50s.

Please rewrite the paragraph on page 29, lines 1-8 as shown:

B15

Any value note can be copied or distributed without increasing the liability of the bank, since the bank only has to honour the first valid presentation of a value note endorsed with payment instructions and a correct signature. The bank cannot avoid honouring at least one presentation, since it will not be able to demonstrate any other payment instructions except those correctly endorsed with the bearer's signature. If the bank is queried over the disposal of any issued note, the bank will be able to issue confirmation copies of the receipt value note 67 (Fig. 11), the seller's value note 50s (Fig. 9) and the buyer's replacement value note 60b (Fig. 10) without increasing its liability.

Please rewrite the paragraph on page 30, lines 19-27 as shown:

B16

In the above, the "valid from" information in the new value notes 50s and 60b may simply represent the instantaneous date and/or time of issuance, as a record of the date and/or time of issuance. Alternatively, the "valid from" information of one or both of the new value notes 50s and 60b may be set a predetermined interval after the time and/or date of

B16 Cont

issuance. This is equivalent to "post-dating" the value note so that it cannot be used again for immediate redemption. A possible advantage of this is that it can prevent a malicious user from repeatedly submitting new value notes for redemption immediately after issuance, and thereby try to overload the bank's computers. The interval may, for example, be from a few minutes, or less, to a day, or longer, as desired.

Please rewrite the paragraph on page 31, lines 8-14 as shown:

B17

Referring to Fig. 12, the buyer appends payment instruction information 100 to the endorsed original value note 67 (Fig. 11), in a similar manner to that described previously. However, the payment instruction information 98 instructs the bank computer 10 to create a only temporary value note 99 (i.e. an option note) having a limited life. The payment instruction information further includes a delayed instruction that, if the option note is not redeemed by the seller by an expiry date selected by the buyer, then the bank computer is to return the funds by issuing a second value note to the buyer.

Please rewrite the paragraph on page 31, lines 19-32 as shown:

B18

Before the buyer sends the endorsed value note 67 and the new blank value notes to the bank, the buyer appends further information to the seller's blank value note 50s (Fig. 9) to transform it into a blank "option" note 101. Referring to Fig. 13, the buyer adds option note information 102 about any further conditions or requirements which the seller must meet before the option note can be redeemed by the seller. Examples of such conditions are described below. The buyer may also

include the expiry date information 104 for the option note (although these could also be included by the bank computer 10 (Fig. 1) later if desired). Finally, the buyer calculates a signature 106 based at least on the option note information 102 to endorse the option note information and prevent this from being altered later. As indicated in Fig. 13, the signature 106 may also be based on other information in the option note 101, such as the seller's public key 52, the value 54 of the option note, and the expiry date 104, to protect these other items of information. As explained previously, a reduced set of information may be used, consisting mainly of the redemption instructions, instead of returning a complete value note.

B18 cont

Please rewrite the paragraph on page 32, lines 1-3 as shown:

B19

The buyer then transmits the modified seller's value note (i.e. the blank option note 101 in Fig. 13) with the endorsed value note 67 and the buyer's two blank value notes, to the bank computer 10 (Fig. 1).

Please rewrite the paragraph on page 32, lines 5-8 as shown:

B20

Fig. 14 illustrates the completed value note 103 which the bank computer 10 (Fig. 1) returns to the buyer. This is similar to that shown in Fig. 11, and includes an "OK" message 94, and a final bank signature 96 to "sign off" the value note 103.

Please rewrite the paragraph on page 33, lines 6-12 as shown:

B21

Fig. 17 illustrates an endorsed option note 111 which includes both of the above examples of option note information. The value note includes a signature 112 calculated by the seller to endorse the option note information 102, or at least a receipt string part of the option note information. In this embodiment, the receipt string comprises encrypted text so that neither the bank computer 10 nor bank staff can read the receipt text. This provides absolute anonymity for the transaction at the same time as providing a receipt decipherable by the buyer and seller.

Please rewrite the paragraph on page 34, lines 1-5 as shown:

B22

When the blinded message T, the signature S and the accompanying information M' and F are sent to the bank computer, the bank computer can verify that the signature is valid by verifying that S = (M' ^ F) mod N. In this manner, the bank can verify that the seller has signed the message to the buyer, even though the bank is not able directly to read the blinded message T.

Please rewrite the paragraph on page 34, lines 16-20 as shown:

B23

The endorsed option note also includes a second signature 114 calculated by the buyer, to meet the requirement in the option note information 102. The buyer's second signature should be calculated using text information if the option note different is from that protected already by the buyer's endorsing signature 106. In this embodiment, the

B23 cont

buyer's second signature is based on text comprising the bank's issuing signature 26.

Please rewrite the paragraph on page 35, lines 10-14 as shown:

B24

After step 122, the bank computer proceeds to step 124 at which bank computer 10 tests whether the option note conditions include a requirement for the seller to endorse a text message (for example, an encrypted receipt message) with the seller's signature. If not, the routine branches past step 126 to indicate that the option note conditions have been met. If a seller's signature is required, step 126 tests whether it matches the receipt text provided by the buyer.

Please rewrite the paragraph on page 35, lines 20-26 as shown:

B25

After the expiry date of the option note, the buyer may contact the bank computer 10 to enquire about the option note. For example, the buyer may submit a copy of the option note as evidence of authorization. If the seller has not redeemed the option note, the bank computer 10 can issue the new value note to the buyer at that stage to return the funds. On the other hand, if the seller has redeemed the option note, then the bank computer can provide a copy of the fully signed option note (Fig. 17) to the original buyer as a receipt for the transaction (which includes the receipt information presented in the option note information 102).

Please rewrite the paragraph on page 36, lines 10-18 as shown:

B26

A further advantage is that if the buyer prepares one or more option notes in advance of potential transactions, the transactions can be performed "off-line" from the bank computer. The buyer may, for example, print each of the one or more option notes on paper, and send or hand the option note to the seller. The seller will then have a certain period (for example, a few days) to make contact with the bank computer to redeem the option note (which is guaranteed up to that time). However, if for any reason the buyer decides not to proceed with any of the transactions and keeps the option notes for those transactions, the bank will simply return the funds to the buyer by issuing new value notes when the option notes expire. In this case, the seller never obtains the option notes.

Please rewrite the paragraph on page 37, lines 4-8 as shown:

B27

Another application for option notes is for a secure transaction, by swapping option notes in such a way that neither party can interrupt the process at some stage whereby they would be able to keep both option notes. In this example, one note may be for currency, and the other note may represent merchandise, such as a value note representation of a share certificate, currency, or an agreement to provide certain goods or services on demand.

Please rewrite the paragraph on page 38, lines 5-13 as shown:

B28

Another example of secure swapping or transacting value notes is described below. In this example, instead of two option notes being used, only one option note is required. However, in order to redeem the option note, one party has to provide evidence that the "swap" value note has been issued, by providing the bank's signature for the "swap" value note. This example also illustrates how option notes can require signatures from other parties even though those parties may not be directly involved in the current value note transaction. The normal use of such signatures is to confirm that certain actions have taken place, e.g. between other parties, or being confirmed by another party, before the option note can be redeemed.

Please rewrite the paragraph on page 43, line 28 through page 44, line 6 as shown:

B29

An alternative technique, illustrated in Fig. 20, is to use a short-hand notation to identify or list each value note, and to include common information, including a single instruction message, in a single message block. This is particularly suitable for value notes which have the same public key. The single message block can consist of:

(a) list of serial numbers of notes to be consolidated

(b) list of values of the notes (this is optional since the values will be known to the bank, but is preferred to reduce the chances of discrepancies after the consolidated note has been issued);

(c) single instruction message, including the basic details for the new, blank value note (i.e. new serial number (or at least the bearer's part of the serial number), public key information for the new note);